

Improve the Maximum Transmission Distance of Four-State Continuous Variable Quantum Key Distribution by using a Noiseless Linear Amplifier

Bingjie Xu^{1,2,*}, Chunming Tang², Hui Chen^{1,2}, Wenzheng Zhang^{1,2}, and Fuchen Zhu^{1,2}

1. Science and Technology on Security Communication Laboratory, 610041, Cheng Du, China

2. Institute of Southwestern Communication, 610041, Cheng Du, China

(Dated: October 2, 2012)

A modified four-state CVQKD protocol is proposed to increase the maximum transmission distance and tolerable excess noise in the presence of Gaussian lossy and noisy channel by using a noiseless linear amplifier (NLA). We show that a NLA with gain g can increase the maximum admission losses by $20 \log_{10} g$ dB.

PACS numbers: 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Quantum key distribution (QKD) provides a means of sharing a secret key between two parties (Alice and Bob) securely in the presence of an eavesdropper (Eve) [1, 2]. The single-photon (e. g. BB84 [3]), entanglement-based (e. g. E91 [4]) and continuous variable (e. g. GG02 [5]) QKD protocols have proved to be unconditionally secure under some (e. g. source, detection, and post-processing) assumptions [1]. In the continuous-variable QKD (CVQKD) protocols, information is encoded in quadratures of coherent or squeezed states, and decoded by homodyne or heterodyne detections [5–8], which have the advantage of only requiring off-the-shelf telecom components [9]. Besides experimental demonstrations [10, 11], the theoretical security of CVQKD has been established against general collective Gaussian attacks [12–15], which has been shown optimal in the asymptotical limit [16]. Furthermore, the effect of finite size has been recently investigated in CVQKD protocol [17–19].

Developing QKD protocol resistant to loss and noise is of great practical importance. The CVQKD protocol based on Gaussian modulation of coherent state has been proven to be technically practical [9]. However, due to the low reconciliation efficiency for correlated Gaussian variables at low SNR (signal to noise ratio), the maximum transmission distance of CVQKD is quite limited [11]. There are two possible ways to solve this problem. One is to build good reconciliation algorithms with reasonable efficiency even at low SNR for Gaussian modulation protocols, where steady progress has been made in recent years [20]. The other is to use discrete modulation CVQKD [21–24], such as the four-state protocol [22, 23], which has been proved to be secure against collective attacks and have large enough reconciliation efficiency at low SNR.

Recently, it is very interesting to see that one can improve the maximum transmission distance of Gaussian modulation CVQKD protocols dramatically by using a nondeterministic noiseless linear amplifier (NLA) [25]. Lately, a method was proposed to improve the secret key rate of four-state CVQKD protocol over long distance by using a phase-sensitive or phase-insensitive optical amplifier, while the maximum trans-

mission distance is decreased [26]. Inspired by the methods in [25], we show that the maximum transmission distance and tolerable excess noise of the four-state CVQKD protocol can be increased by using a NLA before Bob's detection in the presence of a lossy and noisy Gaussian channel. Similar to the result in [25], we find that a NLA with gain g can increase the maximum admissible losses by a factor of g^{-2} . Because of the nondeterministic nature of the NLA, the security proof here is similar to that in CVQKD protocols with post-selection.

II. THE FOUR-STATE CVQKD PROTOCOL

In this section, we firstly describe the prepare-and-measure (PM) and entanglement-based (EB) version of the four-state CVQKD protocol. Then, the secure key rate for the protocol under collective attack is given in detail.

A. The PM and EB description of four-state CVQKD protocol

In the PM version of the four-state CVQKD protocol [22], Alice sends randomly one of the four coherent states $|\alpha_k\rangle = |\alpha e^{i\pi(2k+1)/4}\rangle$, $k = 0, 1, 2, 3$ with probability $1/4$ to Bob through a quantum channel, where α is chosen to be a real positive number. Bob measures randomly one of the quadratures in homodyne detection, and decodes the information by the sign of his measurement result.

The PM version of the four-state CVQKD protocol can be reformulated in EB version. Alice initially prepare a two-mode entangled state

$$|\Phi_{AB}(\alpha)\rangle = \frac{1}{2} \sum_{k=0}^3 |\psi_k\rangle_A |\alpha e^{i(2k+1)\pi/4}\rangle_B, \quad (1)$$

where

$$|\psi_k\rangle = \frac{1}{2} \sum_{m=0}^3 e^{i(1+2k)m\pi/4} |\phi_m\rangle \quad (k = 0, 1, 2, 3) \quad (2)$$

*xbjpk@pku.edu.cn

is a non-Gaussian orthogonal state, and

$$\begin{aligned} |\phi_k\rangle &= \frac{e^{-\alpha^2/2}}{\sqrt{\lambda_k}} \sum_{n=0}^{\infty} (-1)^n \frac{\alpha^{4n+k}}{\sqrt{(4n+k)!}} |4n+k\rangle, \\ \lambda_{0,2} &= \frac{1}{2} e^{-\alpha^2} [\cosh(\alpha^2) \pm \cos(\alpha^2)], \\ \lambda_{1,3} &= \frac{1}{2} e^{-\alpha^2} [\sinh(\alpha^2) \pm \sin(\alpha^2)]. \end{aligned}$$

Then Alice performs a projective measurement $\{|\psi_0\rangle\langle\psi_0|, |\psi_1\rangle\langle\psi_1|, |\psi_2\rangle\langle\psi_2|, |\psi_3\rangle\langle\psi_3|\}$ on mode A to project mode B on one of the four coherent states $|\alpha_k\rangle$ ($k = 0, 1, 2, 3$) randomly, which are then measured by a homodyne detector at Bob's side after passing through a quantum channel.

Although the EB version does not correspond to the actual implementation, it is fully equivalent to the PM version from the a secure point of view [22, 23], and it provides a powerful description of establishing security proof against collective attacks through the covariance matrix γ_{AB} of the state before their respective measurements [25, 26].

B. Secure key rate of four-state CVQKD protocol

The covariance matrix $\gamma_{A_0B_0}$ of the state $|\Phi_{AB}(\alpha)\rangle$ is

$$\gamma_{A_0B_0} = \begin{bmatrix} V\mathbb{I} & Z\sigma_z \\ Z\sigma_z & V\mathbb{I} \end{bmatrix}, \quad (3)$$

where $\mathbb{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, $V = 2\alpha^2 + 1 = V_A + 1$ is variance of quadratures for mode A and B, and

$$Z = 2\alpha^2(\lambda_0^{3/2}\lambda_1^{-1/2} + \lambda_1^{3/2}\lambda_2^{-1/2} + \lambda_2^{3/2}\lambda_3^{-1/2} + \lambda_3^{3/2}\lambda_0^{-1/2}) \quad (4)$$

reflects the correlation between mode A and mode B. After mode B passing through a Gaussian channel with transmittance T and equivalent excess noise at the input ϵ , the quantum state $|\Phi_{AB}(\alpha)\rangle$ turns to state ρ_{AB} with covariance matrix

$$\gamma_{AB}(\alpha, T, \epsilon) = \begin{bmatrix} V\mathbb{I} & \sqrt{T}Z\sigma_z \\ \sqrt{T}Z\sigma_z & T(V + \chi)\mathbb{I} \end{bmatrix}, \quad (5)$$

where $\chi = \frac{T}{1-T} + \epsilon$ is the equivalent total noise at the input. This matrix contains all the information needed to establish the secret key rate for collective attacks for the four-state CVQKD protocol, and the lower bound of secure key rate with reverse reconciliation is [22]

$$R(\alpha, T, \epsilon) \geq \beta I_{AB}(\alpha, T, \epsilon) - S_{BE}(\alpha, T, \epsilon), \quad (6)$$

where

$$I_{AB}(\alpha, T, \epsilon) = \frac{1}{2} \log_2 \left(\frac{V + \chi}{1 + \chi} \right) = \frac{1}{2} \log_2(1 + \text{SNR}) \quad (7)$$

refers here to the mutual information between Alice and Bob [26], S_{BE} is the Holevo bound for the mutual information shared by Eve and Bob, and $\beta < 1$ is the reconciliation

efficiency ($\beta > 0.8$ can be reached for arbitrary low SNR in the four-state CVQKD protocol [22, 23]). As shown in [22], S_{BE} is maximized when the state ρ_{AB} shared by Alice and Bob is a Gaussian state, which means S_{BE} is upper bounded by the same quantity computed for a Gaussian state ρ_{AB}^G with the same covariance matrix as the state ρ_{AB} in an EB version of the protocol [23]. Clearly, one has

$$S_{BE} \leq S_{BE}^G = G\left(\frac{v_1 - 1}{2}\right) + G\left(\frac{v_2 - 1}{2}\right) - G\left(\frac{v_3 - 1}{2}\right), \quad (8)$$

where $G(x) = (x + 1) \log_2(1 + x) + x \log_2 x$, and

$$v_{1,2} = \sqrt{\frac{1}{2}(\Delta \pm \sqrt{\Delta^2 - 4D})} \quad (9)$$

are the symplectic eigenvalues of the covariance matrix γ_{AB} where $\Delta = V^2 + T^2(V + \chi)^2 - 2TZ^2$ and $D = (TV^2 + TV\chi - TZ^2)^2$ [23, 26], and

$$v_3 = \sqrt{V(V_A + 1 - \frac{TZ^2}{TV_A + 1 + T\epsilon})}. \quad (10)$$

is the symplectic eigenvalues of $\gamma_{A|B}$ which corresponds to the covariance matrix of Alice's state given the result of Bob's homodyne measurement [23]. Finally, the lower bound of secure key rate is

$$\underline{R}(\alpha, T, \epsilon) = \beta I_{AB}(\alpha, T, \epsilon) - S_{BE}^G(\alpha, T, \epsilon) \leq R(\alpha, T, \epsilon). \quad (11)$$

III. MODIFIED FOUR-STATE CVQKD PROTOCOL BY USING A NLA

Inspired by the method in [25], we propose a modified four-state CVQKD protocol by using a NLA as shown in Fig. 1(a), where Alice and Bob implement the original four-state CVQKD protocol as usual but Bob adds a NLA before his homodyne detection, which is here assumed to be perfect for simplify of analysis as in [25].

A NLA can in principle probabilistic amplify the amplitude of a coherent state while retaining the initial level of noise [27–31]. The successful amplification can be described by an operator $\hat{C} = g^{\hat{n}}$, where \hat{n} is the photon number operator. When a NLA succeeds amplifying a coherent state,

$$\hat{C}|\alpha\rangle = e^{\frac{|g|^2}{2}(g^2-1)}|g\alpha\rangle, \quad (12)$$

where g is the amplitude gain of a NLA. In the modified four-state CVQKD protocol, only the events corresponding to a successful amplification will be used to extract a secret key, while the other events are aborted. Since the secure key rate of the protocol depends only on the covariance matrix γ_{AB} , it is sufficient to compute it in presence of the NLA to estimate the lower bound of secure key rate $\underline{R}^g(\alpha, T, \epsilon, g)$ corresponding to successfully amplified events.

In the following, we will analysis the performance of the modified four-state CVQKD protocol in two cases: (I) a lossy Gaussian channel without excess, where one can see directly the effect of the NLA; (II) a lossy and noisy Gaussian channel, which is a general and practical case.

A. Case I: Lossy Gaussian channel without excess noise ($\epsilon = 0$)

After mode B passing through a lossy Gaussian channel with transmittance T and no excess noise ($\epsilon = 0$), the state $|\Phi_{AB}\rangle$ turns to $|\Phi'_{AB}\rangle = \frac{1}{2} \sum_{k=0}^3 |\psi_k\rangle | \sqrt{T} \alpha_k \rangle$ with covariance matrix

$$\gamma_{AB}(\alpha, T, \epsilon = 0) = \begin{bmatrix} V\mathbb{I} & \sqrt{T}Z\sigma_z \\ \sqrt{T}Z\sigma_z & T(V + \frac{1-T}{T})\mathbb{I} \end{bmatrix}. \quad (13)$$

Then a NLA with gain g is added to amplify the input state at Bob's side on mode B, which can be described by the operator $g^{\hat{n}}$ when the input state is successfully amplified. One can easily derive that

$$g^{\hat{n}} |\Phi'_{AB}\rangle = \frac{1}{2} e^{\frac{T}{2}|\alpha|^2(g^2-1)} \sum_{k=0}^3 |\psi_k\rangle |g \sqrt{T} \alpha_k\rangle. \quad (14)$$

After the normalization of the output state, the successfully amplified quantum state is $|\Phi''_{AB}\rangle = \frac{1}{2} \sum_{k=0}^3 |\psi_k\rangle |g \sqrt{T} \alpha_k\rangle$ with covariance matrix

$$\gamma_{AB}^g(\alpha, T, \epsilon = 0) = \begin{bmatrix} V\mathbb{I} & \sqrt{g^2 T} Z \sigma_z \\ \sqrt{g^2 T} Z \sigma_z & g^2 T (V + \frac{1-g^2 T}{g^2 T}) \mathbb{I} \end{bmatrix}. \quad (15)$$

One can find that the covariance matrix $\gamma_{AB}^g(\alpha, T, \epsilon = 0)$ corresponds to successful amplification is equal to the covariance matrix $\gamma_{AB}(\alpha^g = \alpha, \eta = g^2 T, \epsilon^g = 0)$ of an equivalent system with $|\Phi_{AB}(\alpha^g)\rangle$ sent through a channel with transmittance $\eta = g^2 T$ and excess noise $\epsilon^g = 0$, without using a NLA (as shown in Fig. 1(b)). Since the lower bound of secure key rate under collective attacks is completely determined by the covariance matrix shared by Alice and Bob, the lower bound of secret key rate $\underline{R}^g(\alpha, T, \epsilon = 0)$ corresponding to the successful amplified events is

$$\underline{R}^g(\alpha, T, \epsilon = 0) = \underline{R}(\alpha, g^2 T, \epsilon = 0), \quad (16)$$

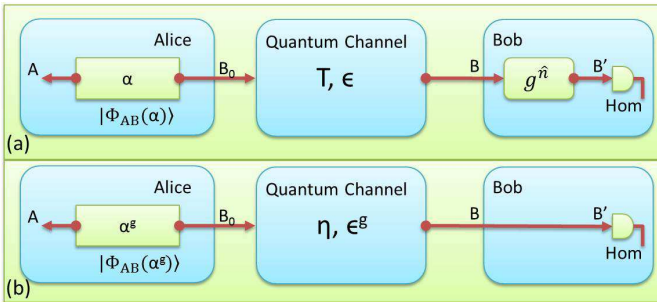


FIG. 1: (color online) (a) Modified four-state CVQKD protocol and (b) virtually equivalent protocol in EB version. A state $|\Phi_{AB}(\alpha)\rangle$ sent through a Gaussian channel with transmittance T and excess noise ϵ , followed by a successful amplification, has the same covariance matrix γ_{AB} than a state $|\Phi_{AB}(\alpha^g)\rangle$ sent through a Gaussian with transmittance η and excess noise ϵ^g without the NLA. The lower bound of secret key rate corresponding to successful amplified events in the modified four-state protocol $\underline{R}^g(\alpha, T, \epsilon)$ is the same as that of the virtually equivalent protocol $\underline{R}(\alpha^g, \eta, \epsilon^g)$.

and the lower bound of total secure key rate is

$$\underline{R}_{tot}^g(\alpha, T, \epsilon) = P_{success} \underline{R}^g(\alpha, T, \epsilon), \quad (17)$$

where $P_{success}$ is the probability of successful amplification by a NLA. A direct conclusion is that a NLA with amplitude gain g can increase the maximum admissible losses of the four-state CVQKD protocol by a factor g^{-2} without excess noise, which is equivalent to improve the maximum transmission distance by $\frac{20 \log_{10} g}{a}$ km, where $a = 0.2 \text{ dB/km}$ for the fiber channel.

B. Case II: Lossy and noisy Gaussian channel ($\epsilon > 0$)

After passing through a Gaussian channel with transmittance T and excess noise ϵ , the state $|\Phi_{AB}(\alpha)\rangle$ turns to ρ_{AB} with covariance matrix

$$\gamma_{AB}(\alpha, T, \epsilon) = \begin{bmatrix} V\mathbb{I} & \sqrt{T}Z\sigma_z \\ \sqrt{T}Z\sigma_z & T(V + \frac{1-T}{T} + \epsilon)\mathbb{I} \end{bmatrix}, \quad (18)$$

where the quantum state of mode B is $\rho_B = \frac{1}{4}(\rho_0 + \rho_1 + \rho_2 + \rho_3)$ with variance $T(V + \frac{1-T}{T} + \epsilon)$.

The ρ_k is the state received by Bob if he knows Alice's measurement result on mode A is k , which can be described by a displaced thermal state

$$\rho_k = D(\beta_k) \rho_{th}(\lambda) D(-\beta_k) = D(\sqrt{T} \alpha_k) \rho_{th}(\lambda) D(-\sqrt{T} \alpha_k), \quad (19)$$

where $\rho_{th}(\lambda) = (1 - \lambda^2) \sum_{n=0}^{\infty} \lambda^{2n} |n\rangle \langle n|$ is a thermal state with variance

$$V(\lambda) = \frac{1 + \lambda^2}{1 - \lambda^2} = 1 + T\epsilon \quad (20)$$

corresponds to Bob's variance when $V_A = 0$. Then a NLA with gain g is added to amplify the input state at Bob's side on mode B. Following the methods in [25], one can derive the effect of a NLA on the displaced thermal state ρ_k ($k = 0, 1, 2, 3$). The P-function of a thermal state with parameter λ is

$$\rho_{th}(\lambda) = \int \frac{1 - \lambda^2}{\pi \lambda^2} e^{-\frac{1-\lambda^2}{\lambda^2} |\alpha'|^2} |\alpha'\rangle \langle \alpha'| d\alpha'. \quad (21)$$

A displacement operation $D(\beta)$ will turn a thermal state to

$$\rho(\beta) = D(\beta) \rho_{th}(\lambda) D(-\beta) = \int \frac{1 - \lambda^2}{\pi \lambda^2} e^{-\frac{1-\lambda^2}{\lambda^2} |\alpha' - \beta|^2} |\alpha'\rangle \langle \alpha'| d\alpha' \quad (22)$$

The effect of a NLA on displaced thermal state $\rho(\beta)$ is

$$\begin{aligned} \rho^g(\beta) &= \hat{C} \rho(\beta) \hat{C} = \int \frac{1 - \lambda^2}{\pi \lambda^2} e^{-\frac{1-\lambda^2}{\lambda^2} |\alpha' - \beta|^2} g^{\hat{n}} |\alpha'\rangle \langle \alpha'| g^{\hat{n}} d\alpha' \\ &= \int \frac{1 - \lambda^2}{\pi \lambda^2} e^{-\frac{1-\lambda^2}{\lambda^2} |\alpha' - \beta|^2 + |\alpha'|^2 (g^2 - 1)} |g\alpha'\rangle \langle g\alpha'| d\alpha'. \end{aligned} \quad (23)$$

By introducing $u = g\alpha'$, one gets

$$\begin{aligned} \rho^g(\beta) &= \int \frac{1 - \lambda^2}{g^2 \pi \lambda^2} e^{-\frac{1-\lambda^2}{\lambda^2} \left| \frac{u}{g} - \beta \right|^2 + |u|^2 \frac{g^2 - 1}{g^2}} |u\rangle \langle u| du \\ &= C \int e^{-\frac{1-\lambda^2}{g^2 \lambda^2} \left| u - g\beta \right|^2 + |u|^2 \frac{1-\lambda^2}{1-g^2 \lambda^2}} |u\rangle \langle u| du, \end{aligned} \quad (24)$$

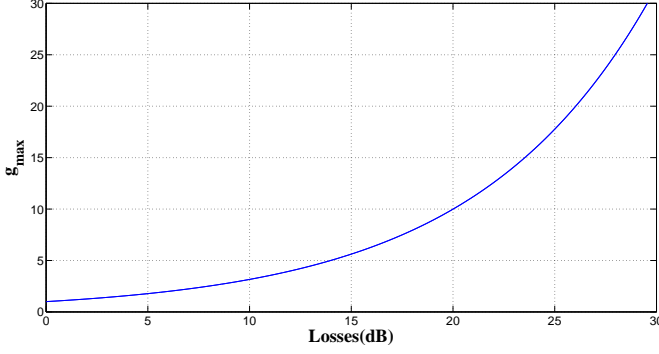


FIG. 2: (color online) The maximum value of the gain of NLA g_{\max} against the losses when $\epsilon = 0.02$.

where C is a global unimportant normalization factor independent of the integrated variable u . The Eq. (24) clearly correspond to a thermal state $\rho_{th}(g, \lambda)$ displaced by $g \frac{1-\lambda^2}{1-g^2\lambda^2} \beta$. Thus, the successful amplification of ρ_k corresponds to a new displaced thermal state ρ_k^g ,

$$\rho_k^g = D(g \frac{1-\lambda^2}{1-g^2\lambda^2} \beta_k) \rho_{th}(g, \lambda) D(-g \frac{1-\lambda^2}{1-g^2\lambda^2} \beta_k), \quad (25)$$

where $\beta_k = \sqrt{T} \alpha_k$. Finally, the action of the NLA on the input state at Bob's side introduce the transformations

$$\sqrt{T} \alpha_k \rightarrow g \frac{1-\lambda^2}{1-g^2\lambda^2} \sqrt{T} \alpha_k, \lambda^2 \rightarrow g^2 \lambda^2, \quad (26)$$

which is equivalent to

$$\sqrt{T} \alpha_k \rightarrow \frac{2g}{2-(g^2-1)T\epsilon} \sqrt{T} \alpha_k, \frac{T\epsilon}{2+T\epsilon} \rightarrow g^2 \frac{T\epsilon}{2+T\epsilon}. \quad (27)$$

In the next step, one need to consider the action of NLA when Bob does not know Alice's measurement result. In such a case, the input state of the NLA is

$$\rho_B = \frac{1}{4}(\rho_0 + \rho_1 + \rho_2 + \rho_3), \quad (28)$$

with variance $1 + T\epsilon + TV_A = \frac{1+\lambda^2}{1-\lambda^2} + 2T\alpha^2$. The output state corresponding to successful amplified events on ρ_B is

$$\rho_{B'} = \frac{1}{4}(\rho_0^g + \rho_1^g + \rho_2^g + \rho_3^g), \quad (29)$$

with variance $\frac{1+g^2\lambda^2}{1-g^2\lambda^2} + 2g^2(\frac{1-\lambda^2}{1-g^2\lambda^2})^2 T\alpha^2$. Thus, the action of the NLA on the input state at Bob's side introduce the transformations

$$\frac{1+\lambda^2}{1-\lambda^2} + 2T\alpha^2 \rightarrow \frac{1+g^2\lambda^2}{1-g^2\lambda^2} + 2g^2\left(\frac{1-\lambda^2}{1-g^2\lambda^2}\right)^2 T\alpha^2, \quad (30)$$

which can be derived from Eq. (27).

Now we want to find a virtual two-mode entangled state $|\Phi_{AB}(\alpha^g)\rangle$, sent through a channel of transmittance η and excess noise ϵ^g without using the NLA, while share the same covariance matrix as $\gamma_{AB}^g(\alpha, T, \epsilon)$ as shown in Fig. 1(b). The following conditions should be satisfied

$$\sqrt{\eta} \alpha^g = g \frac{2}{2-(g^2-1)T\epsilon} \sqrt{T} \alpha, \quad (31)$$

$$\frac{\eta \epsilon^g}{2 + \eta \epsilon^g} = g^2 \frac{T\epsilon}{2 + T\epsilon}, \quad (32)$$

$$1 + \eta \epsilon^g + 2\eta \alpha^{g^2} = \frac{1 + g^2 \lambda^2}{1 - g^2 \lambda^2} + 2g^2 \left(\frac{1 - \lambda^2}{1 - g^2 \lambda^2} \right)^2 T\alpha^2, \quad (33)$$

where the third line can be derived by the first two lines. So, one only need to consider the conditions in Eqs. (31) and (32). Remind that one always has $\alpha^g = \alpha$ for $\epsilon = 0$ or $g = 1$, so we add a third condition

$$\alpha^g = \alpha. \quad (34)$$

Then the solutions for Eqs. (31), (32), and (34) is

$$\eta = \frac{4g^2 T}{[2 + (1 - g^2)T\epsilon]^2}, \epsilon^g = \epsilon - \frac{1}{2}(g^2 - 1)T\epsilon^2, \alpha^g = \alpha. \quad (35)$$

Those parameters can be interpreted as physical parameters of an equivalent system if they satisfy the physical meaning constrains $0 \leq \eta \leq 1$ and $\epsilon^g \geq 0$, which require

$$g_{\max}(T, \epsilon) = \begin{cases} \frac{1}{\sqrt{T}}, & \epsilon = 0 \\ -\frac{2\sqrt{T} + \sqrt{4T + 4T\epsilon(2+T\epsilon)}}{2T\epsilon}, & \epsilon > 0 \end{cases}$$

which is plotted in Fig. 2. Finally, one has

$$\underline{R}^g(\alpha, T, \epsilon) = \underline{R}(\alpha, \eta, \epsilon^g), \quad (36)$$

$$\underline{R}_{tot}^g(\alpha, T, \epsilon) = P_{success} \underline{R}^g(\alpha, T, \epsilon). \quad (37)$$

IV. NUMERICAL SIMULATION AND DISCUSSION

In the following, the performance of the modified four-state protocol is compared with the original one for a given channel with the same transmittance T and excess noise ϵ . The secure key rate of the original protocol is given by $\underline{R}(\alpha, T, \epsilon)$ in Eq. (11), and that of modified protocol is given by $\underline{R}_{tot}^g(\alpha, T, \epsilon)$ in Eq. (37). In numerical simulations, $P_{success}$ is assumed to be a constant, which is reasonable when $\beta < 1$ [25]. The precise value of $P_{success}$ depends on practical implementations. However, it is not not important for our result, since it only acts as a scaling factor of $\underline{R}_{tot}^g(\alpha, T, \epsilon)$ and does not change the fact that a negative secret rate $\underline{R}(\alpha, T, \epsilon)$ can become positive $\underline{R}_{tot}^g(\alpha, T, \epsilon)$ with a NLA for a certain distance of transmission distance. As shown in [25], the value of $P_{success}$ is upper bounded by $1/g^2$, and we choose the value $P_{success} = 1/g^2$ to optimize the performance of the modified four-state CVQKD protocol.

The numerical simulations of $\underline{R}_{tot}^g(\alpha, T, \epsilon)$ and $\underline{R}(\alpha, T, \epsilon)$ with the same channel parameters T and ϵ is shown in Fig. 3,

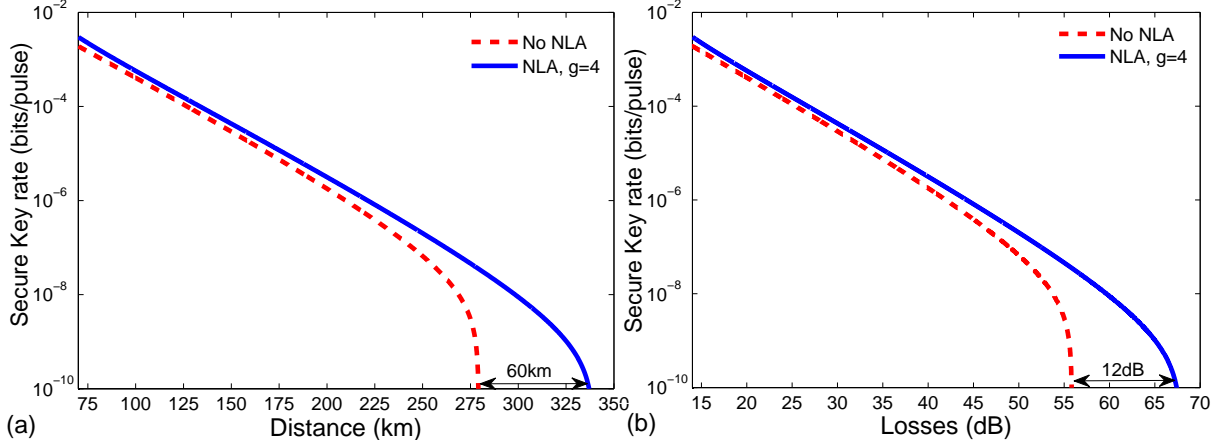


FIG. 3: (color online) (a). The lower bound of secret key rate for the modified four-state CVQKD protocol with a NLA $\underline{R}_{tot}^g(\alpha, T, \epsilon)$ and that of the original protocol without a NLA $\underline{R}(\alpha, T, \epsilon)$ against the transmission distance in *km*. (b). The lower bound of secret key rate for the modified four-state CVQKD protocol with a NLA $\underline{R}_{tot}^g(\alpha, T, \epsilon)$ and that of the original protocol without a NLA $\underline{R}(\alpha, T, \epsilon)$ against the losses in *dB*. In the simulations, $V_A = 2\alpha^2 = 0.25$, $\epsilon = 0.002$, $\beta = 0.8$, $g = 4$, and $P_{success} = 1/g^2$.

where the amplitude gain of the NLA is $g = 4$ and the excess noise is $\epsilon = 0.002$. Similar to the results in [25], one can find that the maximum admissible losses is increased by $20 \log_{10} g$ by using a NLA with gain g , which is equivalent to increase the maximum transmission distance by $\frac{20 \log_{10} g}{0.2}$ km in fiber channel. This result does not depend on the value of $P_{success}$. Even for a more realistic probability of success, the NLA increase the maximum transmission distance in the same way. To test the efficiency for different values of g , the secret key rate for the modified four-state CVQKD protocol with a NLA with gain $g = 2, 3, 4$ is compared with that of the original protocol, as shown in Fig. 4.

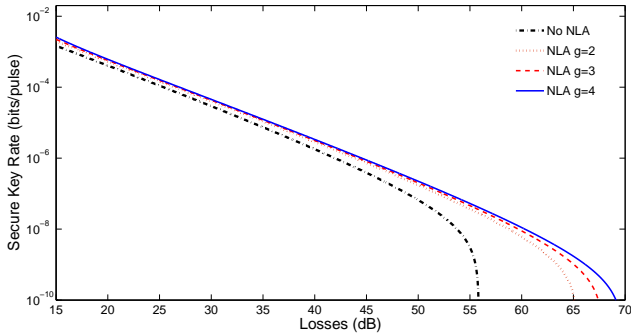


FIG. 4: (color online) The lower bound of the secret key rate for the modified four-state CVQKD protocol with a NLA $\underline{R}_{tot}^g(\alpha, T, \epsilon)$ for $g = 2, 3, 4$ and that of the original protocol without a NLA $\underline{R}(\alpha, T, \epsilon)$ against the losses in *dB*. In the simulations, $V_A = 2\alpha^2 = 0.25$, $\epsilon = 0.002$, $\beta = 0.8$, and $P_{success} = 1/g^2$.

The maximal tolerable excess noise ϵ_{max} for the modified four-state CVQKD protocol by using a NLA with gain g and that of the original protocol is shown in Fig. 5. By using a

NLA, the maximal tolerable excess noise can be increased, and this result does not depend on the value of $P_{success}$.

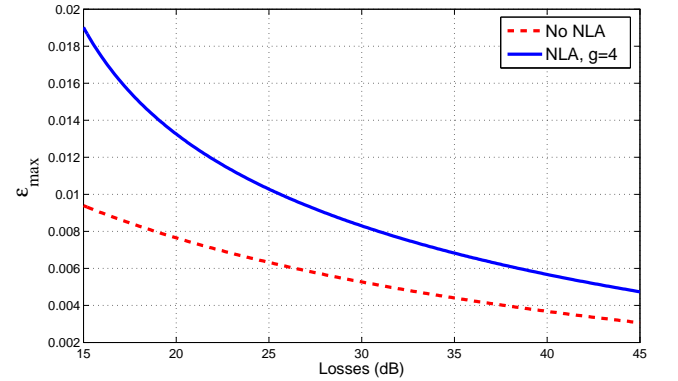


FIG. 5: (color online) Maximal excess noise for the modified and original four-state CVQKD protocol against losses in *dB*. In the simulations, $V_A = 2\alpha^2 = 0.25$, $\beta = 0.8$, $g = 4$, and $P_{success} = 1/g^2$.

V. CONCLUSION

In this paper, a modified four-state CVQKD protocol is proposed. The maximum transmission distance can be increased by the equivalent of $20 \log_{10} g$ dB of losses by using a noiseless linear amplifier before Bob's detection. The modified protocol is also more robust against excess noise.

Steady progress on the experimental realization of the NLA has been made in recent years [27–31]. A further work would be analyzing the gaps between practical implementations and theoretical description of NLA, and the effect of the imperfection on the secure key rate.

This work is supported by Foundation of Science and Technology on Communication Security Laboratory (Grants No.

9140c11010110c1104).

-
- [1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Düsek, N. Lütkenhaus, and M. Peev, *Rev. Mod. Phys.* **81**, 1301 (2009).
 - [2] H. K. Lo and Y. Zhao, *Encyclopedia of Complexity and Systems Science*, Vol. 8 (Springer, New York, 2009), pp. 7265-7289.
 - [3] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), p. 175.
 - [4] A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
 - [5] F. Grosshans and P. Grangier, *Phys. Rev. Lett.* **88**, 057902 (2002).
 - [6] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, *Phys. Rev. Lett.* **93**, 170504 (2004).
 - [7] N. J. Cerf, M. Levy, and G. V. Assche, *Phys. Rev. A* **63**, 052311 (2001).
 - [8] R. Garcia-Patron and N. J. Cerf, *Phys. Rev. Lett.* **102**, 130501 (2009).
 - [9] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, *Rev. Mod. Phys.* **84**, 621 (2012).
 - [10] J. Lodewyck, M. Bloch, R. Garcia-Patron, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, *Phys. Rev. A* **76**, 042305 (2007).
 - [11] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, *New Journal of Physics* **11**, 045023 (2009).
 - [12] R. Garcia-Patron and N. J. Cerf, *Phys. Rev. Lett.* **97**, 190503 (2006).
 - [13] M. Navascues, F. Grosshans and A. Acin, *Phys. Rev. Lett.* **94**, 020505 (2006).
 - [14] S. Pirandola, S. L. Braunstein, and S. Lloyd, *Phys. Rev. Lett.* **101**, 200504 (2008).
 - [15] A. Leverrier and P. Grangier, *Phys. Rev. A* **81**, 062314 (2010).
 - [16] R. Renner and J. I. Cirac, *Phys. Rev. Lett.* **102**, 110504 (2009).
 - [17] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, *Phys. Rev. Lett.* **109**, 100502 (2012).
 - [18] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, *Phys. Rev. A* **86**, 032309 (2012).
 - [19] A. Leverrier, F. Grosshans, and P. Grangier, *Phys. Rev. A* **81**, 062343 (2010).
 - [20] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, *Phys. Rev. A* **84**, 062317 (2011).
 - [21] A. Leverrier and P. Grangier, *Phys. Rev. A* **83**, 042312 (2011).
 - [22] A. Leverrier and P. Grangier, *Phys. Rev. Lett.* **102**, 180504 (2009).
 - [23] A. Leverrier and P. Grangier, arXiv: 1002.4083 (2010).
 - [24] J. Yang, B. Xu, X. Peng, and H. Guo, *Phys. Rev. A* **85**, 052302 (2012).
 - [25] R. Blandino, A. Leverrier, M. Barbieri, J. Etessé, P. Grangier, and R. Tualle-Brouri, *Phys. Rev. A* **86**, 012327 (2012).
 - [26] H. Zhang, J. Fang, and G. He, *Phys. Rev. A* **86**, 022338 (2012).
 - [27] F. Ferreyrol, M. Barbieri, R. Blandino, S. Fossier, R. Tualle-Brouri, and P. Grangier, *Phys. Rev. Lett.* **104**, 123603 (2010).
 - [28] F. Ferreyrol, R. Blandino, M. Barbieri, R. Tualle-Brouri, and P. Grangier, *Phys. Rev. A* **83**, 063801 (2011).
 - [29] M. Barbieri, F. Ferreyrol, R. Blandino, R. Tualle-Brouri, and P. Grangier, *Laser Physics Letters* **8**, 411 (2011).
 - [30] A. Zavatta, J. Fiurasek, and M. Bellini, *Nature Photonics* **5**, 52 (2011).
 - [31] G. Y. Xiang, T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, *Nature Photonics* **4**, 316 (2010).